

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-160828

(43)Date of publication of application : 12.06.2001

(51)Int.Cl.

H04L 12/66
G09C 1/00
H04L 9/08
H04L 9/10
H04L 12/46
H04L 12/28
H04L 3/00

(21)Application number : 11-344500

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 03.12.1999

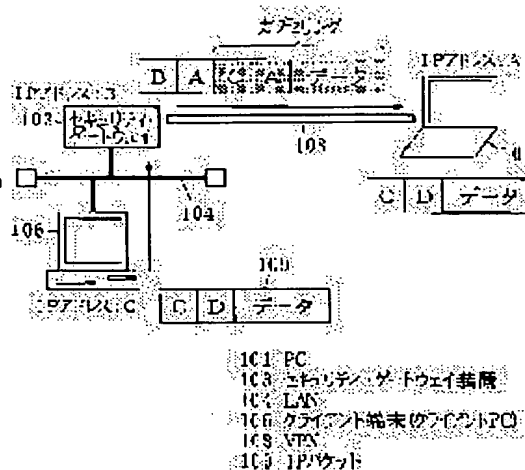
(72)Inventor : MURAKAWA YASUSHI

(54) VPN COMMUNICATION METHOD IN SECURITY GATEWAY DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a VPN communication method for a security gateway device that brings a PC accessed externally via a WAN into a communication enabled state as a virtual terminal under a LAN.

SOLUTION: This invention provides a VPN communication method for the security gateway device 103 that interconnects the WAN consisting of public channels or the like and the LAN 104 through a concentration conversion processing. In the case of realizing a VPN 108 for an external PC 101 connected to the WAN by dialup connection with an IPsec protocol, a DHCP communication option is integrated with IKE data at an IKE communication before the IPsec communication so as to realize designation of a sender IP address C that is IPsec-processed in a tunneled IP packet.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開2001-160828

(P2001-160828A)

(43) 公開日 平成13年6月12日 (2001.6.12)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 12/66		G 0 9 C 1/00	6 6 0 E 5 J 1 0 4
G 0 9 C 1/00	6 6 0	H 0 4 M 3/00	B 5 K 0 3 0
H 0 4 L 9/08		H 0 4 L 11/20	B 5 K 0 3 3
9/10		9/00	6 0 1 B 5 K 0 5 1
12/46			6 2 1 Z 9 A 0 0 1

審査請求 未請求 請求項の数 3 O L (全 7 頁) 最終頁に続く

(21) 出願番号 特願平11-344500

(22) 出願日 平成11年12月3日 (1999.12.3)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 村川 泰

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

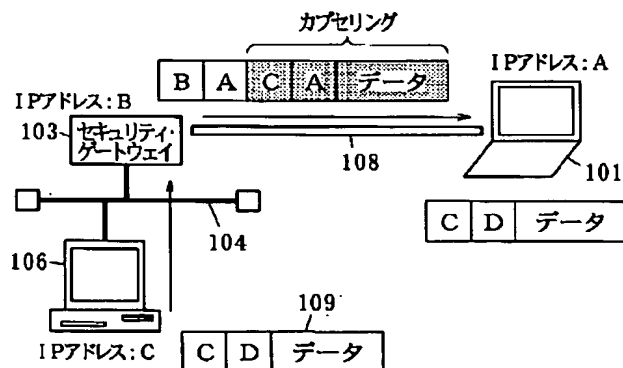
最終頁に続く

(54) 【発明の名称】 セキュリティ・ゲートウェイ装置におけるVPN通信方法

(57) 【要約】

【課題】 WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるVPN通信方法を提供することを目的とする。

【解決手段】 公衆回線などから構成されるWANとLAN 104との間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置 103 におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPC 101 に対してIPsecプロトコルによりVPN 108を実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスCの指定を実現する。



- 101 PC
- 103 セキュリティ・ゲートウェイ装置
- 104 LAN
- 106 クライアント端末 (クライアントPC)
- 108 VPN
- 109 IPパケット

【特許請求の範囲】

【請求項 1】 公衆回線などから構成される WAN と LAN との間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置における VPN 通信方法であって、ダイヤルアップ接続で WAN に接続した外部の PC に対して IPsec プロトコルにより VPN を実現する際、IPsec 通信に先立つ IKE 通信時に、DHCP 通信オプションを IKE データに統合し、トンネリングされた IP パケットにおける IPsec 処理される送信元 IP アドレスの指定を実現するセキュリティ・ゲートウェイ装置における VPN 通信方法。

【請求項 2】 IKE 通信時に、セキュリティ・ゲートウェイ装置配下の LAN と同じセグメントの IP アドレス／サブネットマスクアドレスをダイヤルアップ接続から LAN にアクセスする前記外部の PC に割り当て、前記外部の PC を仮想的に LAN 環境下に置いた VPN 通信を実現する請求項 1 に記載のセキュリティ・ゲートウェイ装置における VPN 通信方法。

【請求項 3】 NAT 技術を組み合わせて前記外部の PC に LAN 配下で使用しているプライベート IP アドレスを IKE 通信時に付与し、プライベート IP アドレスで構築された LAN 環境への前記外部の PC からのアクセスが可能な VPN 通信を実現するセキュリティ・ゲートウェイ装置における VPN 通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、複数の PC を接続した LAN と公衆回線などの WAN (Wide Area Network) とを集線・変換処理を行うことにより接続するセキュリティ・ゲートウェイ装置で構成されるネットワーク環境において、公衆回線にダイヤルアップ接続した外部の PC が WAN を介してセキュリティ・ゲートウェイ装置と VPN (Virtual Private Network、仮想専用網) 通信を行うためのセキュリティ・ゲートウェイ装置における VPN 通信方法に関するものである。

【0002】

【従来の技術】 近年、企業のみならず家庭に至るまで複数台の PC が導入され、インターネットへの接続が進んでいる。複数台の PC で構成される LAN をインターネットに接続する場合、LAN と WAN を接続するゲートウェイ装置が必要になる。また、LAN の外部の PC から LAN 配下の端末にアクセスするには、まず契約しているプロバイダにダイヤルアップ接続し、WAN 経由で LAN 配下の端末 (例えば PC) にアクセスすることになる。

【0003】 しかし、WAN を流れるパケットは基本的に安全性が確保されておらず、パケットを盗聴されると、第三者に通信内容を悪用される恐れがある。通信内容の秘匿性と外部からの不正アクセスを防止するために

は、WAN と LAN を接続するセキュリティ・ゲートウェイ装置が必要となり、ダイヤルアップ接続する PC にもセキュリティのための通信プロトコルスタックが実装されてないといけない。そして、外部からアクセスする PC (外部の PC) とセキュリティ・ゲートウェイ装置の間で VPN 通信を行うことで、WAN 上で仮想的な専用線環境が実現できる。現在、VPN 通信のための代表的な通信プロトコルとして実装されているのは IPsec (Security Architecture for the Internet Protocol) である。

【0004】 以下に、IPsec を利用した VPN 通信の概要を説明する。まず図 4 を参照しながら説明する。図 4 は WAN を含む一般的なネットワークシステムを示す構成図である。

【0005】 図 4 において、101 はプロバイダにダイヤルアップ接続した外部の PC、102 は WAN、103 は WAN 102 と後述の LAN 104 を接続して集線・変換処理を行うセキュリティ・ゲートウェイ、104 はセキュリティ・ゲートウェイ 103 配下の LAN、105 は LAN 104 上のサーバ端末、106、107 は LAN 104 上のクライアント PC、108 は PC 101 とセキュリティ・ゲートウェイ 103 との間で IPsec 通信を行うために確立された VPN である。

【0006】 ダイヤルアップ接続した PC 101 が LAN 104 上の端末にアクセスする場合、セキュリティ・ゲートウェイ 103 との間で VPN 108 を確立し、WAN 102 上で仮想的な専用線環境を実現する。こうして WAN 102 上で通信内容を盗聴・改竄できないようにし、LAN 104 配下の端末と通信を行う。

【0007】 次に、IPsec 通信を行うために必要な通信内容の概要について図 5 を用いて解説する。図 5 は WAN による接続を示す WAN 接続図である。

【0008】 図 5 において、PC 101、WAN 102、セキュリティ・ゲートウェイ 103 は図 4 と同様のものである。

【0009】 PC 101 とセキュリティ・ゲートウェイ 103 との 2 点間で IPsec 通信を行う場合、データの秘匿性、コネクションレスな完全性 (相手との論理的な通信路を構築せず、データの改ざんを防止すること)、改ざん防止などを保証するための暗号アルゴリズム、認証アルゴリズムに用いる鍵情報を両者が IPsec 通信を行う前に共有できてないといけない。両者で鍵情報を共有させる方法として、事前に両者で鍵情報を手動で設定する方法と、IKE (Internet Key Exchange) プロトコルを用いて自動設定する方法の 2 通りがある。ここでは、現実的な方法である IKE プロトコルによる自動鍵情報交換方式のみを適用する。

【0010】 次に、図 6 を用いて IPsec 通信につい

3

て説明する。図6はIPsec通信開始のためのセキュリティ・ゲートウェイ103の動作を示すフローチャートである。

【0011】IPsec通信を行うためには、2点間で双方向に論理的なコネクションSA (Security Association) を確立しなければならない。そのためにIKE通信は2つのフェーズに分かれていて、フェーズ1において安全なIKE通信を行うためのIKE-SAを確立しようとし(S11、S12)、

4

それに成功したら、フェーズ2において、IPsec通信するための鍵情報などのセキュリティ情報を交換する(S13)。フェーズ2でIPsec-SAを確立することができれば(S14)IKE通信を終了し、IPsec通信が開始する(S15)。ステップS13のIKE (フェーズ2) 通信においてIPsec通信を行うために2点間で交換される情報を(表1)に示す。

【0012】

【表1】

項 目	詳 細
セキュリティ・プロトコル	ESP/AH
IPsec通信モード	トンネルモード/トランスポートモード
暗号アルゴリズム	ESPの場合必須
暗号鍵	—
認証アルゴリズム	AHの場合必須、ESPでも選択可
認証鍵	—
SAの寿命形式	データ量(バイト)/時間(量)
SAの寿命	—

【0013】但し動作モード(IPsec通信モード)については、セキュリティ・ゲートウェイ103はトンネルモード(IPパケット全体をカプセリングする)でしか動作できないので、ここでは、IPsecの動作モードはトンネルモードのみを想定する。

【0014】図7はトンネルモードのIPsec通信の概要を示す説明図である。

【0015】図7において、PC101、セキュリティ・ゲートウェイ103、LAN104、クライアントPC106、VPN108は図4と同様のものである。100はIPパケットである。

【0016】図7において、PC101、セキュリティ・ゲートウェイ103、クライアントPC106のIPアドレスをそれぞれA、B、Cとする(AはプロバイダによってPC101に付与されたIPアドレス)。LAN104上のクライアントPC106からVPN108を介してコネクションの張られたPC101にIPパケットを送信する場合、まずクライアントPC106において、送信元IPアドレスがC、宛先IPアドレスがAのIPパケット100が作成され、送信される。セキュリティ・ゲートウェイ103がこのパケット100を受信し、VPN108を張られたPC101宛てのパケットであることを識別すると、IKE通信による交換した情報に基づいてIPパケット100をカプセリングする。元のIPアドレスの外側に、送信元IPアドレスB、宛先IPアドレスAのIPヘッダが付加される。このとき交換した情報に基づいてカプセリングされたIP

パケットへの認証情報の付加、暗号化が行われる。VPN108を介してカプセリングされたパケットを受信したPC101は、交換した情報に基づいてカプセリングされた元のIPパケット100を取り出し、処理する。

【0017】

【発明が解決しようとする課題】しかしながら、上記従来のセキュリティ・ゲートウェイ装置におけるVPN通信方法では、WAN102上でのデータの安全性は確保できているが、あくまで外部ネットワークからのアクセスと判断されるため、LAN104配下のクライアントPC106の情報にアクセスするために、LAN104配下のクライアントPC106に設定(アクセス許可/不許可を示すセキュリティ・ポリシーの設定、例えば許可するIPアドレスと不許可となるプロトコル・サービスなど)が必要になり、その設定のために別の安全性の問題が生じる可能性があり、LAN104がプライベートIPアドレスで構成されたネットワークの場合、その設定は特に困難になるという問題点を有していた。

【0018】このセキュリティ・ゲートウェイ装置におけるVPN通信方法では、WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にすることが要求されている。

【0019】本発明は、この要求を満たすため、WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるVPN通信方法を提供することを目的とする。

【0020】

【課題を解決するための手段】この課題を解決するために本発明のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、公衆回線などから構成されるWANとLANとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPCに対してIPsecプロトコルによりVPNを実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定を実現する構成を備えている。

【0021】これにより、WANを介して外部からアクセスするPCを仮想的にLAN配下の端末として通信可能にするセキュリティ・ゲートウェイ装置におけるVPN通信方法が得られる。

【0022】

【発明の実施の形態】本発明の請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、公衆回線などから構成されるWANとLANとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPCに対してIPsecプロトコルによりVPNを実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定を実現することとしたものである。

【0023】この構成により、セキュリティ・ゲートウェイ装置は、ダイヤルアップ接続した外部のPCとIPsec通信する際、そのPCの最終的な宛先IPアドレスを制御可能にし、LAN配下の端末への設定を不要とし、安全性が確保されるという作用を有する。

【0024】請求項2に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法において、IKE通信時に、セキュリティ・ゲートウェイ装置配下のLANと同じセグメントのIPアドレス／サブネットマスクアドレスをダイヤルアップ接続からLANにアクセスする外部のPCに割り当て、外部のPCを仮想的にLAN環境下に置いたVPN通信を実現することとしたものである。

【0025】この構成により、VPNを確立した外部のPCがLAN環境内にあるように仮想的にみなせる作用を有する。

【0026】請求項3に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法は、請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法において、NAT技術を組み合わせて外部のPCにLAN配下で使用しているプライベートIPアドレスをI

KE通信時に付与し、プライベートIPアドレスで構築されたLAN環境への外部のPCからのアクセスが可能なるVPN通信を実現することとしたものである。

【0027】この構成により、プライベートIPアドレスで構成されたLAN環境に、安全性を確保したまま外部のPCからのアクセスを可能にするという作用を有する。

【0028】以下、本発明の実施の形態について、図1～図3を用いて説明する。

10 【0029】（実施の形態1）図3は、本発明の実施の形態1によるセキュリティ・ゲートウェイ装置におけるVPN通信方法において用いるIKE通信データフォーマットを示すフォーマット図である。

【0030】図3に示す通り、IKE通信はUDP (User Datagram Protocol) / IP (Internet Protocol) を使用して行われる。IKEデータは、ISAKMP (Internet Security Association and Key Management Protocol) ヘッダの後にISAKMPペイロードが数珠つなぎの形態で続くことで構成される。IKE通信は、鍵交換を要求する始動者（イニシエータ、Initiator）とそれに対して応答する応答者（レスポンド、Responder）によって行われる。本実施の形態においては、図4において、プロバイダにダイヤルアップしてインターネットに接続したPC101がInitiatorとなり、LAN104上の端末としてのクライアントPC106、107にアクセスするために、セキュリティ・ゲートウェイ103にIKE通信を開始し、セキュリティ・ゲートウェイ103がResponderとしてIKE通信を行う。（表1）に挙げた項目のうち、暗号鍵と認証鍵は、公開鍵暗号方式を用いてInitiatorとResponderの間で鍵情報が交換されるが、それ以外の項目は、Initiatorが提案をし、ResponderがInitiatorの提案の中から最適なものを選択して応答するというサーバ／クライアントモデルで行われる。DHCP (Dynamic Host Configuration Protocol) クライアントとしてのPC101が取得すべき必須の情報として、IPアドレス、サブネットマスク、IPアドレスの有効期限、ドメイン名がある。これら4つの情報をIKE通信においてResponderであるセキュリティ・ゲートウェイ103が通常のIKEデータでオプションとして付加する。但し、IPアドレスの有効期限はIKE通信によって確立されるSAの寿命と同じと考えることで省略することができる。またDHCPもUDPの上位に位置するアプリケーションプロトコルなので、IKEに組み込んでも再送制御その他の問題は起こらない。

50 【0031】図1は本発明の実施の形態1におけるIP

s e c通信の概略を示す説明図である。

【0032】図1において、PC101、セキュリティ・ゲートウェイ103、LAN104、クライアントPC106、VPN108は図4と同様のものである。

【0033】図1において、PC101、セキュリティ・ゲートウェイ103、クライアントPC106のIPアドレスをそれぞれA、B、Cとする（AはプロバイダによってPC101に付与されたIPアドレス）。また、IPsec通信に先立つIKE通信により、セキュリティ・ゲートウェイ103は、PC101にIPアドレスDを配布する。LAN104上のクライアントPC106からVPN108を介してコネクションの張られたPC101にIPパケットを送信する場合、まずクライアントPC106において、LAN104外部でプロバイダによってPC101に割り当てられたIPアドレスAを意識することなく、送信元IPアドレスがC、宛先IPアドレスがDのIPパケット109が作成され、送信される。セキュリティ・ゲートウェイ103がこのパケット109を受信し、VPN108を張られたPC101宛てのパケットであることを識別すると、IKE通信による交換した情報に基づいてIPパケット109をカプセリングする。元のIPアドレスの外側に、送信元IPアドレスB、宛先IPアドレスAのIPヘッダが付加される。このとき交換した情報に基づいてカプセリングされたIPパケットへの認証情報の付加、暗号化が行われる。VPN108を介してカプセリングされたパケットを受信したPC101は、交換した情報に基づいてカプセリングされた元のIPパケット109を取り出し、IKE通信により取得したサブネットマスク、ドメイン名を元にIPパケット109を処理する。

【0034】図2はセキュリティ・ゲートウェイ103がPC101にIPアドレスDを配布する手順を示すフローチャートである。

【0035】IPsec通信を行うためには、2点間で双方向に論理的なコネクションSAを確立しなければならない。そのためにIKE通信は2つのフェーズに分かれていて、フェーズ1において安全なIKE通信を行うためのIKE-SAを確立しようとし（S1、S2）、それに成功したら、フェーズ2において、IPsec通信するための鍵情報などのセキュリティ情報を交換する（S3）。フェーズ2でIPアドレスDを配布し、IPsec-SAを確立することができれば（S4）IKE通信を終了する（S5）。ステップS3のIKE（フェーズ2）通信においてIPsec通信を行うために2点間で交換される情報は（表1）に示す通りである。

【0036】以上のように本実施の形態によれば、ダイヤルアップ接続でWAN102に接続したPC101に対してIPsecプロトコルによりVPN108を実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリ

ングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定（アドレスCの指定）を実現するようにしたことにより、セキュリティ・ゲートウェイ103は、ダイヤルアップ接続した外部のPC101とIPsec通信する際、そのPCの最終的な宛先IPアドレスAを制御可能にし、LAN104配下のクライアント端末106への設定を不要とすることができるので、通信内容の盗聴、改竄のおそれが無くなり、安全性を確保することができる。

10 【0037】（実施の形態2）本発明の実施の形態2によるセキュリティ・ゲートウェイ装置におけるVPN通信方法を図1を用いて説明する。

【0038】図1において、IKE通信のResponderであるセキュリティ・ゲートウェイ103からInitiatorであるPC101にDHCP情報を配布する際に、セキュリティ・ゲートウェイ103配下のLAN104と同じセグメントのIPアドレス、サブネットマスクを配布する。VPN108確立後のIPsec通信において、VPN108上を流れるパケット以外は、LAN104外部から接続するPC101も、セキュリティ・ゲートウェイ103配下のクライアント端末106とネットワークセグメント上区別のない、しかも一意な端末として通信を行う。

【0039】以上のように本実施の形態によれば、IKE通信時に、セキュリティ・ゲートウェイ103配下のLAN104と同じセグメントのIPアドレス/サブネットマスクアドレスをダイヤルアップ接続からLAN104にアクセスするPC101に割り当て、外部のPC101を仮想的にLAN104環境下に置いたVPN通信を実現するようにしたことにより、VPN108を確立した外部のPC101がLAN104環境内にあるように仮想的にみなすことができるので、安全性を確保したまま外部からLAN104内の端末にアクセスすることができる。

【0040】（実施の形態3）本発明の実施の形態3によるセキュリティ・ゲートウェイ装置におけるVPN通信方法を図1を用いて説明する。

【0041】図1において、セキュリティ・ゲートウェイ103がNAT（Network Address Translator）技術を用い、セキュリティ・ゲートウェイ103配下のLAN104をプライベートIPアドレスのみで構成していた場合、通常は外部からLAN104上のクライアント端末106にはアクセスできないが、ダイヤルアップ接続したPC101とセキュリティ・ゲートウェイ103がVPN108を確立するためのIKE通信の中で、セキュリティ・ゲートウェイ103配下のLAN104で使用されているセグメントにおける、まだ使用されていないプライベートIPアドレスをIKEに組み込んだDHCPオプションによりPC101に配布することにより、WAN102上に

あるVPN108上はグローバルIPアドレスで通信しながら、LAN104内、そしてPC101の内部では、プライベートIPアドレスでネットワークセグメント上区別のない、しかも一意な端末として通信を行うことができる。

【0042】以上のように本実施の形態によれば、NAT技術を組み合わせて外部のPC101にLAN104配下で使用しているプライベートIPアドレスをIKE通信時に付与し、プライベートIPアドレスで構築されたLAN104環境への外部からのアクセスが可能なVPN通信を実現するようにしたことにより、プライベートIPアドレスで構成されたLAN104環境に、安全性を確保したまま外部のPC101からのアクセスが可能になる。

【0043】

【発明の効果】以上説明したように本発明の請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法によれば、公衆回線などから構成されるWANとLANとの間を集線・変換処理により接続するセキュリティ・ゲートウェイ装置におけるVPN通信方法であって、ダイヤルアップ接続でWANに接続した外部のPCに対してIPsecプロトコルによりVPNを実現する際、IPsec通信に先立つIKE通信時に、DHCP通信オプションをIKEデータに統合し、トンネリングされたIPパケットにおけるIPsec処理される送信元IPアドレスの指定を実現することにより、セキュリティ・ゲートウェイ装置は、ダイヤルアップ接続した外部のPCとIPsec通信する際、そのPCの最終的な宛先IPアドレスを制御可能にし、LAN配下の端末への設定を不要とすることができるので、安全性を確保することができるという有利な効果が得られる。

【0044】請求項2に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法によれば、請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法において、IKE通信時に、セキュリティ・ゲートウェイ装置配下のLANと同じセグメントのIPアドレス/サブネットマスクアドレスをダイヤルアップ接続からLANにアクセスする外部のPCに割り当て、外部のPCを仮想的にLAN環境下に置いたVPN通信を実現することにより、VPNを確立した外部のPCがL

AN環境内にあるように仮想的にみなすことができるので、安全性を確保したまま外部からLAN内の端末にアクセスすることができるという有利な効果が得られる。

【0045】請求項3に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法によれば、請求項1に記載のセキュリティ・ゲートウェイ装置におけるVPN通信方法において、NAT技術を組み合わせて外部のPCにLAN配下で使用しているプライベートIPアドレスをIKE通信時に付与し、プライベートIPアドレスで構築されたLAN環境への外部のPCからのアクセスが可能なVPN通信を実現することにより、プライベートIPアドレスで構成されたLAN環境に、安全性を確保したまま外部のPCからのアクセスが可能になるという有利な効果が得られる。

【図面の簡単な説明】

【図1】本発明の実施の形態1におけるIPsec通信の概略を示す説明図

【図2】セキュリティ・ゲートウェイが外部のPCにIPアドレスを配布する手順を示すフローチャート

【図3】本発明の実施の形態1によるセキュリティ・ゲートウェイ装置におけるVPN通信方法において用いるIKE通信データフォーマットを示すフォーマット図

【図4】WANを含む一般的なネットワークシステムを示す構成図

【図5】WANによる接続を示すWAN接続図

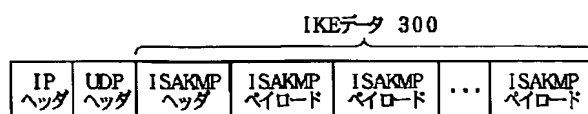
【図6】IPsec通信開始のためのセキュリティ・ゲートウェイ装置の動作を示すフローチャート

【図7】トンネルモードのIPsec通信の概要を示す説明図

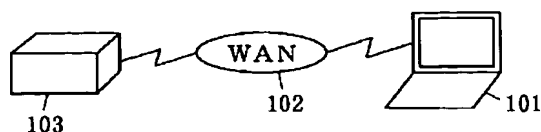
【符号の説明】

101 PC
102 WAN
103 セキュリティ・ゲートウェイ
104 LAN
105 サーバ端末
106、107 クライアント端末（クライアントPC）
108 VPN
109 IPパケット

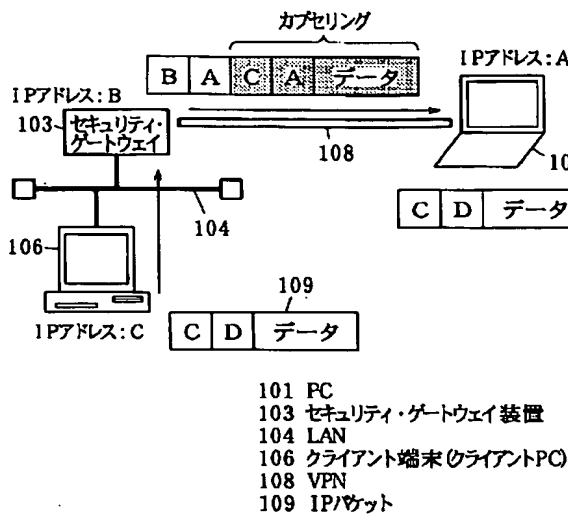
【図3】



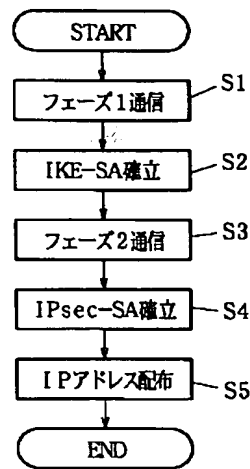
【図5】



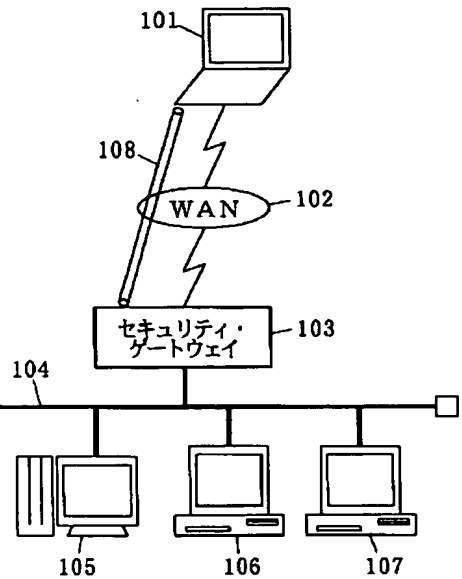
【図1】



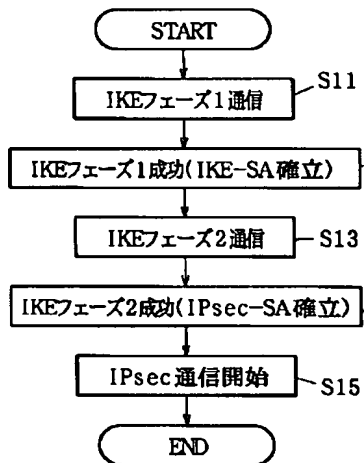
【図2】



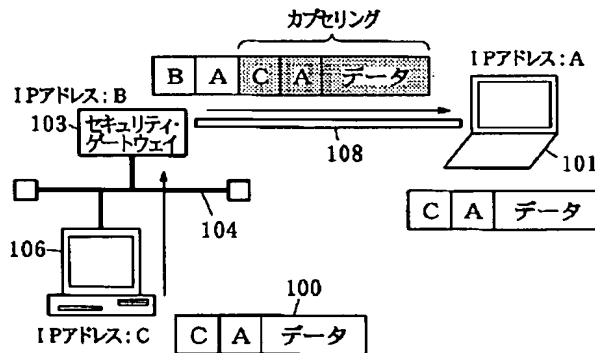
【図4】



【図6】



【図7】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テーマコード(参考)

H 0 4 L 12/28

H 0 4 L 11/00

3 1 0 C

H 0 4 M 3/00

Fターム(参考) 5J104 AA01 AA16 EA01 EA04 JA21

NA02 PA07

5K030 GA15 HC01 HC13 HD03 HD08

HD09 LD19

5K033 BA04 CB08 DA06 DB14 DB18

5K051 BB02 CC01 GG02 HH18

9A001 CC08 JJ25 LL03

THIS PAGE BLANK (USPTO)